IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE
OBTAINED FROM GOVERNMENT'S USE OF CELL SITE SIMULATOR

Okello Chatrie, through counsel, moves the Court to suppress evidence that law enforcement officers obtained pursuant to a warrant authorizing the government to use a cell site simulator. The officers illegally obtained data pursuant to this warrant listed in the search warrant return that remains under seal as indicated below. The Court must suppress those items listed in the search warrant return.

I. Factual basis for the motion.

A bank robbery happened at the Call Federal Credit Union in Midlothian, Virginia on May 20, 2019. Using a series of warrants, all of which started from a state search warrant being challenged in this case, law enforcement officials identified Mr. Chatrie as a possible suspect in the robbery. The officers sought and obtained a warrant to seize a sweeping amount of information pursuant to a warrant they obtained to operate a cell site simulator. The officers executing the warrant seized data pursuant to the warrant.[1] Because the search warrant, the search warrant

[1] The government has provided the defense with a redacted copy of this search warrant with no explanation as to why the redaction is necessary in this case. This search warrant remains sealed. *See In re Search of Use of a Cell-Site Simulator*, 3:19sw210 (E.D. Va. July 17, 2019). As the sealing order which the government provided to the defense does not allow for any disclosure (even to the defense) until further order, Mr. Chatrie does not attach it here. As the defense does not know what information is being redacted,

application, and the return remain under seal at this time, the defense does not attach them here, but all of these documents are available to the Court in *In re Search of Use of a Cell-Site Simulator*, 3:19sw210 (E.D. Va. July 17, 2019).

A cell site simulator is a class of surreptitious cell phone surveillance devices.[2] These privacy-invasive devices have been employed by law enforcement agencies for years with little to no oversight from legislative bodies or the courts due to an intentional policy of secrecy.[3] Cell site simulators can be carried by hand, installed in vehicles, or mounted on aircraft.[4] The devices masquerade as the cellular tower antennas used by wireless companies such as AT&T and Sprint, and in doing so, force all mobile phones within the range of the device that subscribe to the impersonated wireless carrier to emit identifying signals, which can be used to locate not only a particular suspect, but bystanders as well. That is what happened in this case.

II. Use of the cell site simulator violated the Fourth Amendment.

a. Cell site simulator technology is both invasive and precise.

Wireless carriers provide coverage through a network of base stations, also known as "cell sites," that connect cell phones to the telephone network. Cell site simulator models masquerade as a wireless carrier's base station, prompting all wireless devices within range that use the

---

the defense reserves the option to provide additional bases for the challenge to this warrant once the defense can see an unredacted copy of the warrant application.

[2] These devices have a variety of names, including "Stingray," "TriggerFish," "KingFish," and "Hailstorm." *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013, available at http://bit.ly/1mkumNf (last visited Oct. 22, 2019). StingRays, Hailstorms, and other models of cell site simulators are also called "IMSI catchers," in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track. *See* Stephanie K. Pell & Christopher Soghoian, Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy, 28 Harv. J.L. & Tech. 1, 11 (2014).

[3] *See* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today, Aug. 24, 2015, available at http://usat.ly/1LtSLdI (last visited Oct. 22, 2019).

[4] *Gallagher*, supra note 2; *see also* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J., Nov. 13, 2014, *available at* http://on.wsj.com/1EHIEez (last visited Oct. 22, 2019).

impersonated wireless carrier to communicate with it. Depending on the particular features of the device and how the operator configures them, cell site simulators can be used to identify nearby phones, to precisely locate them, and can even block service to devices in the area.[5] Cell site simulators are commonly used by law enforcement agencies in two ways: to collect the unique electronic serial numbers associated with all phones in a given area, or to locate a particular phone "when the officers know the numbers associated with it but don't know precisely where it is."[6]

Some versions of the technology can also obtain metadata about a suspect's calls and text messages or even the contents of those communications.[7] Cell site simulators locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength and direction of those transmissions until the target phone is pinpointed. This dynamic is essential to understanding the Fourth Amendment status of cell site simulator technology. As explained by the U.S. Department of Justice and numerous other sources, "[c]ell-site simulators . . . function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device . . . transmit signals to the simulator." Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology [hereinafter "DOJ Guidance"] 2 (Sept. 3, 2015), available at http://www.justice.gov/opa/file/767321/download (last visited Oct. 22, 2019); *accord In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015) ("[T]he device causes or forces cell-phones

[5] *See* Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, Wired, Mar. 1, 2015, available at http://bit.ly/1K5Aa76 (last visited Oct. 22, 2019).
[6] Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011), available http://on.wsj.com/1D2IWcw (last visited Oct. 22, 2019).
[7] Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired, Oct. 28, 2015, available athttp://bit.ly/1PRCGQC (last visited Oct. 22, 2019).

in an area to send their signals—with all the information contained therein—to the cell-site simulator."). In other words, the cell site simulator device used in this case did not passively intercept the signals transmitted between Mr. Chatrie's phone and Sprint's network, but rather forced Mr. Chatrie's phone to transmit information to the government that it would not otherwise have transmitted to the government.

Accordingly, the "third-party doctrine," as set out in *Smith v. Maryland*, 442 U.S. 735 (1979), and *Upshur v. State*, 208 Md. App. 383 (2012), is inapposite. Those cases involved law enforcement obtaining information from third-party phone companies that was already in the companies' possession. Unlike the dialed phone numbers transiting the phone company's network in *Smith* and the subscriber information held in the phone company's files in *Upshur*, the location information in this case was obtained by a law enforcement officer directly from Mr. Chatrie's phone. When the police seek information by directly interacting with a suspect's phone, no third party is involved, and the Fourth Amendment warrant requirement applies. Just as the Fourth Amendment regulates police use of a thermal imaging camera to remotely obtain information about heat signatures emanating from a home, *Kyllo v. United States*, 533 U.S. 27, 34 (2001), so too does it regulate use of a cell site simulator to solicit and receive data from a cell phone. Both involve direct collection of information by police, not requests for data already held by a third party.

For the following reasons, use of a cell site simulator constitutes a search within the meaning of the Fourth Amendment. First, the devices transmit invisible, probing electronic signals that penetrate walls of Fourth Amendment-protected locations, including homes, offices, and other private spaces occupied by the target and innocent third parties in the area. Cell site simulators force cell phones within those spaces to transmit data to the government that they would not

otherwise reveal to the government, and allow agents to determine facts about the phone and its location that would not otherwise be ascertainable without physical entry. By pinpointing suspects and third parties while they are inside constitutionally protected spaces, cell site simulators invade reasonable expectations of privacy. *See Kyllo*, 533 U.S. at 34 (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of radio-location beeper that was taken into residence constituted search).[8]

Second, the devices can pinpoint an individual with extraordinary precision, in some cases "with an accuracy of 2 m[eters]." Just as in this case, in cases across the country, law enforcement agents have used cell site simulators to pinpoint suspects' locations not only in free-standing houses, but even in specific apartments or areas within large apartment complexes. *See, e.g., State v. Tate*, 849 N.W.2d 798, 804 (Wis. 2014); *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013); Tr. of Suppression Hr'g 14, 17, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010), available at http://bit.ly/1jYUgUT (last visited Oct. 22, 2019). In one Baltimore case, police reportedly used a cell site simulator to determine even that the person carrying the target phone was riding on a particular bus.[9] Accurate electronic location tracking of this type requires a warrant because it intrudes on reasonable expectations of privacy. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (noting Fourth Amendment implications of cell phone location data that can "reconstruct someone's specific

[8] Indeed, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). In this situation, "[t]he [cell site simulator] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate.'" *Kyllo*, 533 U.S. at 38. To protect such intimate details, "the Fourth Amendment draws 'a firm line at the entrance to the house.'" *Id.* at 39.

[9] Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014, available at http://bsun.md/1uE8k7v (last visited Oct. 22, 2019).

movements down to the minute, not only about town but also within a particular building"); *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgement) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *Tracey*, 152 So.3d at 526 ("[T]he use of [a suspect's] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required."); *State v. Earls*, 70 A.3d 630, 586 (N.J. 2013) (tracking a cell phone "can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so.").

Third, cell site simulators search the contents of people's phones by forcing those phones to transmit their electronic serial number and other identifying information held in electronic storage on the device, as well as the identity of the (legitimate) cell tower to which the phone was most recently connected and other stored data. *See* Stipulation, *United States v. Harrison*, No. 14 Cr. 170 (D. Md. Nov. 7, 2014), ECF No. 32-1 ("The simulator can also collect radio signals containing the channel and cell-site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting."). As the Supreme Court held, searching the contents of a cell phone requires a warrant. *Riley*, 134 S. Ct. 2473.

Fourth, cell site simulators impact third parties on a significant scale. In particular, they interact with and capture information from innocent bystanders' phones by impersonating one or more wireless companies' cell sites and thereby triggering an automatic response from all mobile devices on the same network in the vicinity. DOJ Guidance at 5.[10] This is so even when the

[10] *See also, e.g.*, Hannes Federrath, *Multilateral Security in Communications*, Protection in Mobile Communications, 5 (1999), available at http://bit.ly/1QHLfwk (last visited Oct. 22, 2019) ("possible to determine the IMSIs of all users of a radio cell"); Daehyun Strobel, Seminararbeit, Ruhr-Universität, IMSI Catcher 13 (July 13, 2007), available at http://bit.ly/1P3dS7i (last visited on Oct. 22, 2019) ("An IMSI

government is using a cell site simulator with the intent to locate or track a particular suspect; collection of innocent bystanders' phone identifying data and location information is inevitable and unavoidable using current cell site simulator technology. Thus, when using a cell site simulator, the police infringe on the reasonable expectations of privacy of large numbers of innocent non-suspects, amplifying the Fourth Amendment concerns.

Finally, cell site simulators can, as a side-effect of their normal use, disrupt the ability of phones in the area to make calls. *See* DOJ Guidance at 5. The Harris Corporation, the company that manufactures several cell site simulators, has apparently taken steps to ensure that 911 calls are not disrupted. However, emergency calls to doctors, psychologists, and family members may be blocked while the cell site simulator is in use nearby. This is invasive in general, raises possible conflicts with federal law, *see* 47 U.S.C. § 333 (prohibiting interference with cellular transmissions), and can have enormous consequences for anyone in an emergency situation trying to make an urgent call for assistance. To avoid effecting an unreasonably invasive or destructive search, *see* United States v. Ramirez, 523 U.S. 65, 71 (1998), use of cell site simulators must be strictly constrained and explicitly authorized by a court.

B. Use of the device violates the Fourth Amendment.

Cell site simulator use raises serious constitutional concerns due to the dragnet nature of the device's surveillance and the collateral impacts of the device's broadcasts on innocent third parties. As discussed above, cell site simulators can collect identifying information about large numbers of innocent bystanders' phones, send electronic signals through the walls of nearby homes and offices, and interfere with bystanders' ability to make and receive phone calls. The

Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in.").

Fourth Amendment was "the product of [the Framers'] revulsion against" "general warrants" that provided British "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). Cell site simulators inevitably interact with and collect data from the phones of innocent third parties as to whom there is no individualized suspicion, let alone probable cause. Authorization for such sweeping surveillance raises the type of concerns that animate the prohibition on general warrants. *See United States v. Leon*, 468 U.S. 897, 899 (1984) ("[A] warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.").

C. The government's application contained material omissions invalidating any purported judicial authorization to use a cell site simulator.

In its application seeking authorization to locate Mr. Chatrie's cell phone, the government omitted crucial information about how such a device operates, the true privacy implications for innocent third parties, and the fact that regular use of the cell site simulator can significantly disrupt phone calls nearby. Unlike a pen register, a cell site simulator does not merely "record," but broadcasts signals that penetrate the walls of every private home in its vicinity and force responses from bystanders' phones.

The government's omissions fail its duty of candor to the courts. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (Kozinski, J. concurring) ("A lack of candor in . . . the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."). When omissions from an application for a court order were "made intentionally or with reckless disregard for accuracy," and where those omissions were material to the court's decision to grant

the order, the order is deemed invalid and derivative evidence must be suppressed. *Yeagy v. State*, 63 Md. App. 1, 8 (1985). The omissions were material here.

By declining to apprise the court of exactly how the cell site simulator works, the government prevented the court from exercising its constitutional function of ensuring that searches are not overly intrusive, that the rights of non-suspects are protected, and that all aspects of the search are supported by probable cause and described with particularity. The need for candor and specificity when seeking court authorization to use a cell site simulator has recently been recognized by the federal Departments of Justice and Homeland Security, which require that "applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used." DOJ Guidance at 5. Had the issuing judge had access to full and accurate information, he likely would have withheld or modified the order, as other fully informed judges have done.

When judges have learned that police departments are seeking to use cell site simulators and have understood the capabilities of those devices, they have limited the scope of orders. In one federal investigation in New Jersey, for example, the government submitted an application for a pen register order to use a cell site simulator. Appl. for Pen Register Order ¶¶ 3–7, *United States v. Williams*, No. 13 Cr. 548, Mag. No. 12-3092 (D.N.J. July 13, 2012), ECF No. 63-8. Based on the government's description, and recognizing that a pen register order cannot authorize electronic surveillance that invades constitutionally protected spaces, the federal magistrate judge reviewing the application modified the government's proposed order to prohibit the FBI from using the cell site simulator "in any private place or where [FBI agents] have reason to believe the Target [phone] is in a private place." Order at 5, *id.*

Other judges have similarly imposed reasonable protections when presented with accurate and full information. After the local newspaper in Charlotte, North Carolina, revealed that police had been using cell site simulators for eight years pursuant to pen register orders, but had not made their intent to do so explicit in their applications, a judge denied an application for such an order, a first for that court.[11] A federal magistrate judge in Illinois recently issued an opinion explaining the importance of courts having full and accurate information about cell site simulator use, and mandating that future cell site simulator warrants require police to minimize collection and retention of bystanders' data. *In re Application*, 2015 WL 6871289 (N.D. Ill. 2015).

Here, had the government properly described to Judge Novak the device and its impact on bystanders, he could have denied the application or imposed limits on use of the device. Federal judges have responded to pen register applications to use a cell site simulator along these lines. *See, e.g.*, *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 201 (C.D. Cal. 1995). The government's omission of material information requires suppression, both because it invalidates the order, and because, even if the order were valid on its own terms, such order simply did not and could not authorize conduct that the government did not present for approval.

CONCLUSION

The Court must find that the warrant was unreasonable in its scope and manner of intrusion. As such, the Court must suppress all evidence gained from the cell site locator.

Respectfully submitted,
OKELLO T. CHATRIE

[11] Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, available at https://www.wbtv.com/story/27473706/cmpds-cellphone-tracking-cracked-high-profile-cases/ (last visited Oct. 22, 2019).

By: _____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on October 22, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org